- Also see Multiple WLANs

Contents

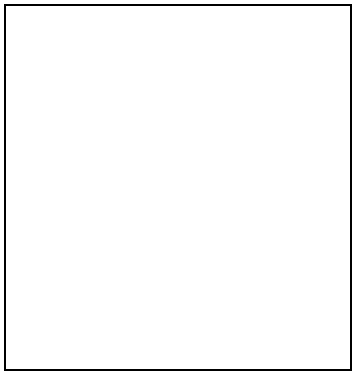
Introduction

This tutorial for beginners provides the basics of creating and controlling a "guest" Wi-Fi Virtual Access Point (VAP) that allows guest users access to the public Internet while keeping them out of your private network.

The following procedures assume the basic setup of the router has been completed and Wi-Fi access to your network is functioning. You should also have determined that the router is capable of simultaneously supporting multiple SSIDs. For a method of checking the revision number of your router's chip and thus its multiple-SSID capability, see https://www.howtogeek.com/153827/how-to-enable-a-guest-access-point-on-your-wireless-network/.

Before proceeding, make sure your router has a working reset button and you have backed up the router's configuration, so if you should get stuck, you can reset it and restore the configuration. (See the **Administration >> Backup** tab in the DD-WRT Control Panel.)

Instructions



Creating Guest VAP

In the **Wireless >> Basic Settings** tab of the DD-WRT Control Panel, click "Add" in the "Virtual Interfaces" section. A new Virtual Interface is created, with a title like

Virtual Interfaces wl0.1 SSID [dd-wrt_vap] HWAddr [22:AA:4B:36:EC:10]

Note the string after "Virtual Interfaces" ("wl0.1" in this example from a Linksys router using a Broadcom chip), as it will help you identify the correct section of later Control Panel pages in which settings will be applied.

Change the Wireless Network Name (SSID) from the default "dd-wrt_vap" to how you want it to appear to guest users when they connect to your network, *e.g.*, "MyNetwork_guest".

Set **AP isolation** to "Enable" so that guest users cannot see each other. AP Isolation drops all traffic between clients connected to the VAP. This is recommended to prevent wireless snooping attacks via the guest Wi-Fi.

Click on the Save button at the bottom of the page. If you do not click the Save button, settings you just made will be lost as you switch from one tab to another.

Go to the **Wireless >> Wireless Security** tab to set the security type and wireless network password. Although the VAP can function with no encryption and password, it can lead to abuse and is thus not recommended. *Click on the Save button at the bottom of the page*.

Set **Network Configuration** to **Unbridged**, **Enable NAT** (gives guests Internet access), and **enable Net isolation** (creates firewall rules blocking guests from the private network). Net isolation works *only* on an unbridged interface on newer builds, *starting from build*:

- Broadcom (23020), Atheros (24759), MediaTek/Ralink (25934)
  AP Isolation = Guests cannot see each other on guest VAP
  Net isolation = Guests cannot see your private LAN+WLAN

Enable Forced DNS Redirection and enter the OpenDNS server IP (208.67.222.222) in the Optional DNS target field. This will prevent users from using their own DNS servers (and hence get around content filtering) by intercepting DNS queries and forcing them to use the DNS servers you specify. Enter the IP Address and Subnet Mask, *e.g.*, 172.16.1.1 / 255.255.255.0. (Private networks use IP addresses in the range 172.16.1.1 to 172.16.1.255.) Click the "Save" button, then click the "Apply" button at the bottom of the page. Wait approximately 30 seconds for the new interface (*e.g.*, wl0.1) to be created.

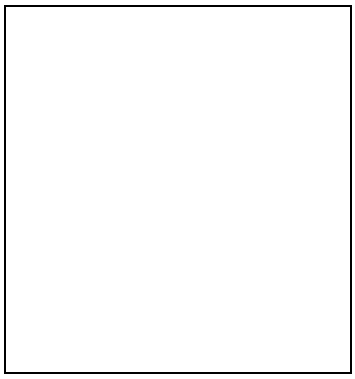
Although this VAP will now show up in a scan of available Wi-Fi access points using your wireless device, you will not yet be able to connect to it. You must enable DHCP for the clients.

Adding DHCP for Guests
Next step is to **enable DHCPd** for the guest Wi-Fi. Go to **Setup >> Networking**, in the *DHCPd* section add a DHCP server for the new guest network (*Add* then choose the VLAN (e.g., ath0.1) from drop down menu. Select starting and max number of IP address, plus lease time. Click *Save* then *Apply*. Wait about 30sec and try to connect to Guest Wi-Fi. If not working, power cycle the router. You should be able to browse the

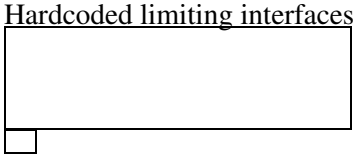
Internet, but not reach your private network nor see other clients on network discovery.

Note: For a newer method that uses DNSMasq instead of DHCPd, see Guest Network § DNSMasq method.

Quality of Service (QoS)



Hardcoded limiting interfaces



Setting priorities

Bandwidth limiting puts the private network on "Maximum" and guest network to "Bulk". The Bulk class is only allocated the remaining bandwidth when other classes are idle. If the pipe is full of traffic from other classes, Bulk will only be allocated 1% of total set limit. This is so your guests will not affect your private network speed. Alternatively, you can manually set hard-coded limits.

Interface limiting, both bridged and unbridged, offers ability to rate-limit or priority-limit services or port(s) ranges. This can be exceptionally useful to control bandwidth hogs, regulate hotspots, etc. with an interface limit, preventing guest users from circumventing QoS limits by changing IP and/or MAC addresses. Abusive users can't bypass your rules without switching off the interface.

Example:

```
vlan1 512/512 0 ssl manual
```

This means all traffic on the vlan1 interface (lan ports for some routers, others use eth) is not limited nor shaped, and goes "up to" global limits, except SSL traffic, being limited to 512 kbps (64 kB/s) both up and down. Multiple entries are also possible, for example:

```
ath0 512/512 0 ssl manual
ath0 2048/512 0 http manual
ath0 512/512 0 ftp manual
```

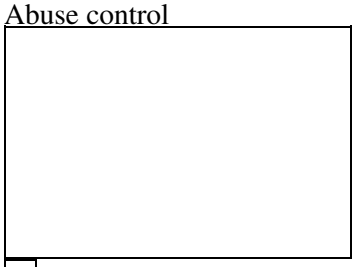
The same applies to what was said above, just for the ath0 wireless interface and only the listed services are rate-limited. Priority limits can also be used, but simultaneous rate limiting and prioritizing on the same service is not supported.

Access Restrictions

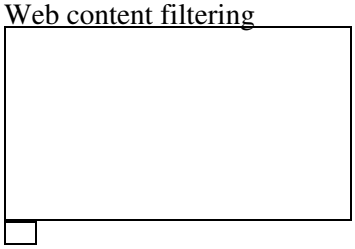
Access Restrictions can be used to block torrents and some VPNs. A determined user is very hard to block, because now there are free SSTP VPN services, etc. On cheap routers you cannot run Proxy, Squid, etc., so to accomplish network abuse filtering we use **OpenDNS**.

OpenDNS

Abuse control



Web content filtering



Content blocked

OpenDNS is a free DNS (Domain Name Server) service to make Internet browsing safer and allegedly faster. By using the OpenDNS DNS server instead of the ISP's DNS server, you are automatically protected from their list of phishing Web sites. However, in order to restrict certain content, *e.g.*, "adult" sites, you will need to create a free account, register your IP address, and select the categories you want restricted ? sexuality, nudity, pornography, lingerie, grotesque, etc. Since most of us have DHCP assigned WAN IP addresses that change periodically, we need to instruct our router to tell OpenDNS the new IP address when it changes. See the DNS-O-Matic section of the OpenDNS article. Reboot router, clear browser cache, and manually set public DNS server in your PC NIC adapter to try to avoid restrictions.

References and notes

<references />